ZRTP Transport Requirements

draft-zimmermann-avt-zrtp-02.txt

Phil Zimmermann <prz@mit.edu>
Alan Johnston <alan@sipstation.com>
Jon Callas <jon@pgp.com>

ZRTP Message Types

- Discovery messages
  - Hello and HelloACK
  - Used to implement Best Effort SRTP
    - Indicates support for ZRTP and ability to have secure media sessions with SRTP
  - Sent at start of every media stream even to non-ZRTP endpoints
- Key Agreement messages
  - Commit, DHPart1, DHPart2, Confirm1, Confirm2, Conf2ACK, GoClear, ClearACK
    - Actual key agreement messages
  - Only sent after discovery exchange
  - Only sent between ZRTP endpoints
  - Contains DH public values approx 8k bits in size

ZRTP Message Requirements

- All Messages
  - Must traverse the maximum number of media intermediaries
  - Need to be sent even for unidirectional and inactive media streams
  - Must not require extensions to signaling protocol beyond current deployed base (i.e. RFC 3261, 4566, etc.)
- Discovery Messages
  - Must be “safe” to send to non-ZRTP endpoints
    - No crashes or disconnects
  - Typically need to be retransmitted due to packet loss
- Key Management Messages
  - Must have simple correlation to a media stream
  - Need exchange to complete in short period

ZRTP is signaling channel/protocol independent

- Faster Deployment
  - Even adding a single signaling extension can delay deployments by years
- Unfortunately the entire Internet doesn't use SIP ;-)
  - ZRTP works with other signaling protocols (H.323, Jingle, etc) as long as they us RTP
- Allows media-only intermediaries
- It is simpler (and possible)

RTP vs. RTCP

- RTP with header extensions meet these requirements
- RTCP with RTP port multiplexing may meet these requirements
  - Safety currently unknown
  - Traversal of intermediaries unknown